

Time to Get Serious About HIPAA

by Bob Radecki

Background

This is the first in a series of articles on the new HIPAA Privacy and Security rules. In this article, we discuss what is changing and the impact these changes could have on health insurance agencies. In the second article we will share common HIPAA mistakes and discuss strategies to comply with the new rules.

A portion of the American Recovery and Reinvestment Act of 2009 (ARRA) called the HITECH Act contains significant changes to HIPAA. Many of the changes will require all covered entities (organizations subject to HIPAA) to update their policies and procedures. Three areas of HITECH, however, are of particular importance to health insurance consultants, brokers and agents.

1. For the first time business associates are directly subject to HIPAA Privacy and Security provisions. Prior to HITECH, brokers were obligated contractually to implement certain procedures when they signed business associate agreements, but were not directly subject to HIPAA. This all changes on February 17th, 2010.
2. Significant changes were made to increase the Department of Health and Human Services (HHS) enforcement of HIPAA.
3. HITECH contains a new breach notification rule that applies to certain privacy or security incidents. Beginning September 24th 2009, covered entities will need to notify effected individuals, the HHS, and sometimes even the media, when a breach occurs. The law also requires business associates to notify their covered entity client of a breach.

Business Associate Directly Subject to HIPAA

An agent often plays the role of a business associate of an employer sponsored health plan. When HIPAA was first passed many brokers signed business associate agreements (BAAs) with employer clients. The terms of these agreements typically require a broker to implement various privacy and security protections. If an agency has already taken steps such as performing a security assessment, implementing written policies and procedures, and conducting employee training in an effort to meet the terms of BAAs, they are well on their way to meeting the full HIPAA requirements.

Unfortunately, in my practice I see many agencies that have entered into business associate agreements, but have done little else and don't even have written privacy and security policies and procedures. That is not to say that they are reckless with their client's information, but let's face it, often clients know even less about HIPAA than agents so until now the threat of a client trying to enforce the business associate agreement has been low.

Beginning in 2010 there is a new sheriff in town. Effective February 27th, 2010 business associates will be directly subject to HIPAA. With this simple change to the law an agency could be directly investigated by HHS or even sued for a HIPAA violation. In light of the HITECH changes many covered entities, including employer groups, are likely to take a more careful look at a broker's compliance with HIPAA. Covered entities may also be asking business associates to sign new BAAs with language that reflect the new legal status of business associates.

Increased Enforcement

Through 2008 HHS's Office for Civil Rights (OCR) has investigated over 9000 HIPAA complaints. In most cases the OCR has resolved the case through a "corrective action" involving voluntary

compliance changes by the organization under investigation. ARAA contains a number of changes which could significantly increase enforcement activity.

- HHS is now required to perform periodic compliance audits.
- In many cases HHS is required by the law to impose penalties. In the past OCR had greater discretion in the imposition of penalties.
- Fines and penalties collected will be used for further enforcement activity.
- In certain circumstances individuals harmed by a violation will be paid a portion of penalties collected.
- State Attorneys General will have the right to pursue some criminal violations of HIPAA

Considering these changes it is reasonable to assume that enforcement of HIPAA violations will increase in the future. Just how much enforcement will change remains to be seen.

The New HIPAA Breach Notification Requirement

The breach notification rule is causing great concern among covered entities and their business associates. The rule requires covered entities and business associates to track all breaches and submit them annually to HHS. Breaches involving more than 500 individuals must be reported to HHS immediately, and in some cases even the public media must be notified. The breach notification rules also require a business associate to notify the covered entity any time there has been a breach. Finally, HHS is required by law to post a list of larger breaches on their website.

It is important to note that not every HIPAA violation meets the definition of a breach. In the interim final regulations released in August, HHS states that an incident must cause a risk of financial or reputational harm to the individual to qualify as a breach. The rules require organizations to perform a risk analysis when there has been a HIPAA violation to determine if the event meets the requirements of a breach. Unfortunately, it is easy to see how a loss or misuse of the kind of client data typically maintained and used by agents could meet this definition.

While organizations have always worried about a HIPAA lawsuit or regulatory action, the thought of having to publically disclose privacy violations strikes fear into the heart of any business person. Many agencies and firms I work with are more worried about the prospect of informing a large employer client of a HIPAA breach than they are of the risk of an HHS investigation. Agencies should implement effective policies and procedures now to reduce the likelihood of a breach, and plan for how to handle a situation where a notice to an employer client is required.

Summary

If an agency has done a good job implementing appropriate HIPAA policies and procedures, now is the time to review them and make any changes necessary to meet the new requirements. If a firm does not have written privacy and security policies, has not trained their workforce, or has not done the security risk assessment required by HIPAA, it is time to take compliance seriously. In the next article of the series we will review common HIPAA mistakes and discuss compliance strategies for insurance agencies. In the meantime more information is available from the HHS at <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html>, or at www.knowhipaa.com.

About The Author

Bob Radecki is currently a Principal at the HR consulting firm of W.J. Flynn and Associates, LLC and manages the HIPAA compliance organization KnowHIPAA.com. Bob has over 25 years experience helping brokers and employers deal with difficult compliance issues. Bob founded and, for over 10 years, served as President of A.E. Roberts Company, a nationally recognized compliance consulting and training firm. Bob was also the principal HIPAA consultant to a number of health insurance companies and has been the featured speaker at many industry events. Bob can be reached at bob.radecki@wjflynnandassociates.com. For more information call 612-581-6281 or go to www.KnowHIPAA.com.